Security on the Desktop

Fighting the Enemy Within

GovTechNet 99-15 June 99

Army Research Laboratory

Adelphi Lab Center (ARL-ALC)

LTC Paul Walczak
(301) 394-3862 DSN 290
pwalczak@arl.mil

Form SF298 Citation Data

Report Date *("DD MON YYYY")* 15061999	**Report Type** N/A	**Dates Covered (from... to)** *("DD MON YYYY")*

Title and Subtitle Security on the Desktop Fighting the Enemy Within	**Contract or Grant Number**
	Program Element Number
Authors	**Project Number**
	Task Number
	Work Unit Number
Performing Organization Name(s) and Address(es) Army Research Laboratory Adelphi Lab Center (ARL-ALC)	**Performing Organization Number(s)**
Sponsoring/Monitoring Agency Name(s) and Address(es)	**Monitoring Agency Acronym**
	Monitoring Agency Report Number(s)
Distribution/Availability Statement Approved for public release, distribution unlimited	
Supplementary Notes	
Abstract	
Subject Terms	
Document Classification unclassified	**Classification of SF298** unclassified
Classification of Abstract unclassified	**Limitation of Abstract** unlimited
Number of Pages 10	

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503

1. AGENCY USE ONLY (Leave blank)

2. REPORT DATE
6/15/99

3. REPORT TYPE AND DATES COVERED
Briefing

4. TITLE AND SUBTITLE
Security on the Desktop, Fighting the Enemy Within

5. FUNDING NUMBERS

6. AUTHOR(S)
LtCol Paul Walczak

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

IATAC
Information Assurance Technology Analysis
Center
3190 Fairview Park Drive
Falls Church VA 22042

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Defense Technical Information Center
DTIC-IA
8725 John J. Kingman Rd, Suite 944
Ft. Belvoir, VA 22060

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION / AVAILABILITY STATEMENT

12b. DISTRIBUTION CODE
A

13. ABSTRACT ***(Maximum 200 Words)***

This briefing entitled “Security on the Desktop: Fighting the Enemy Within” was presented by LTC Paul Walczak, of the Army Research Laboratory to GovTechNet 99 in June 1999. It examines the scope of the challenges of securing Army information and information networks and provides some examination of some of the INFOSEC research areas that will tackle this problem.

14. SUBJECT TERMS
INFOSEC

15. NUMBER OF PAGES

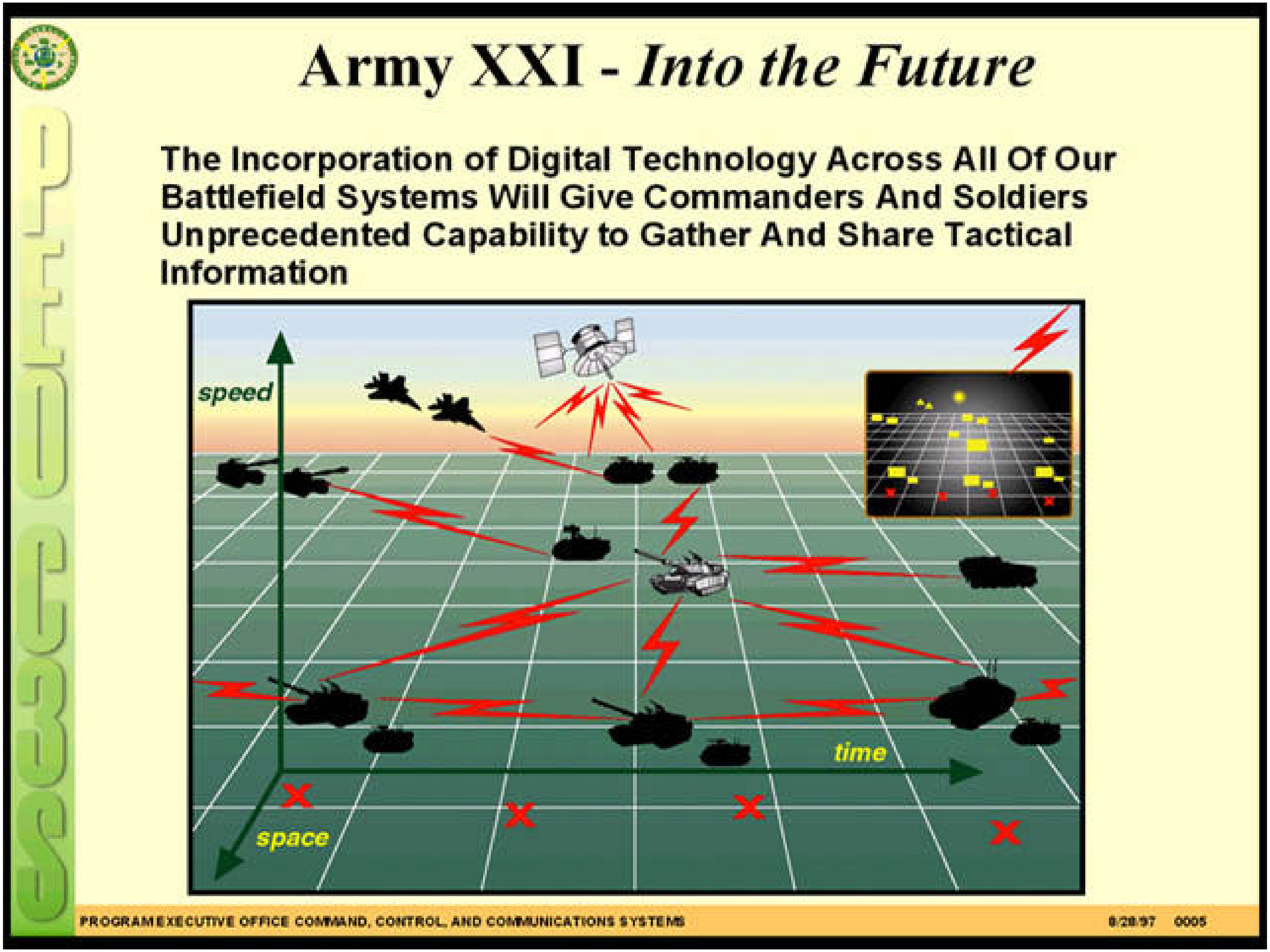
16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT
Unclassified

18. SECURITY CLASSIFICATION OF THIS PAGE
UNCLASSIFIED

19. SECURITY CLASSIFICATION OF ABSTRACT
UNCLASSIFIED

20. LIMITATION OF ABSTRACT
None



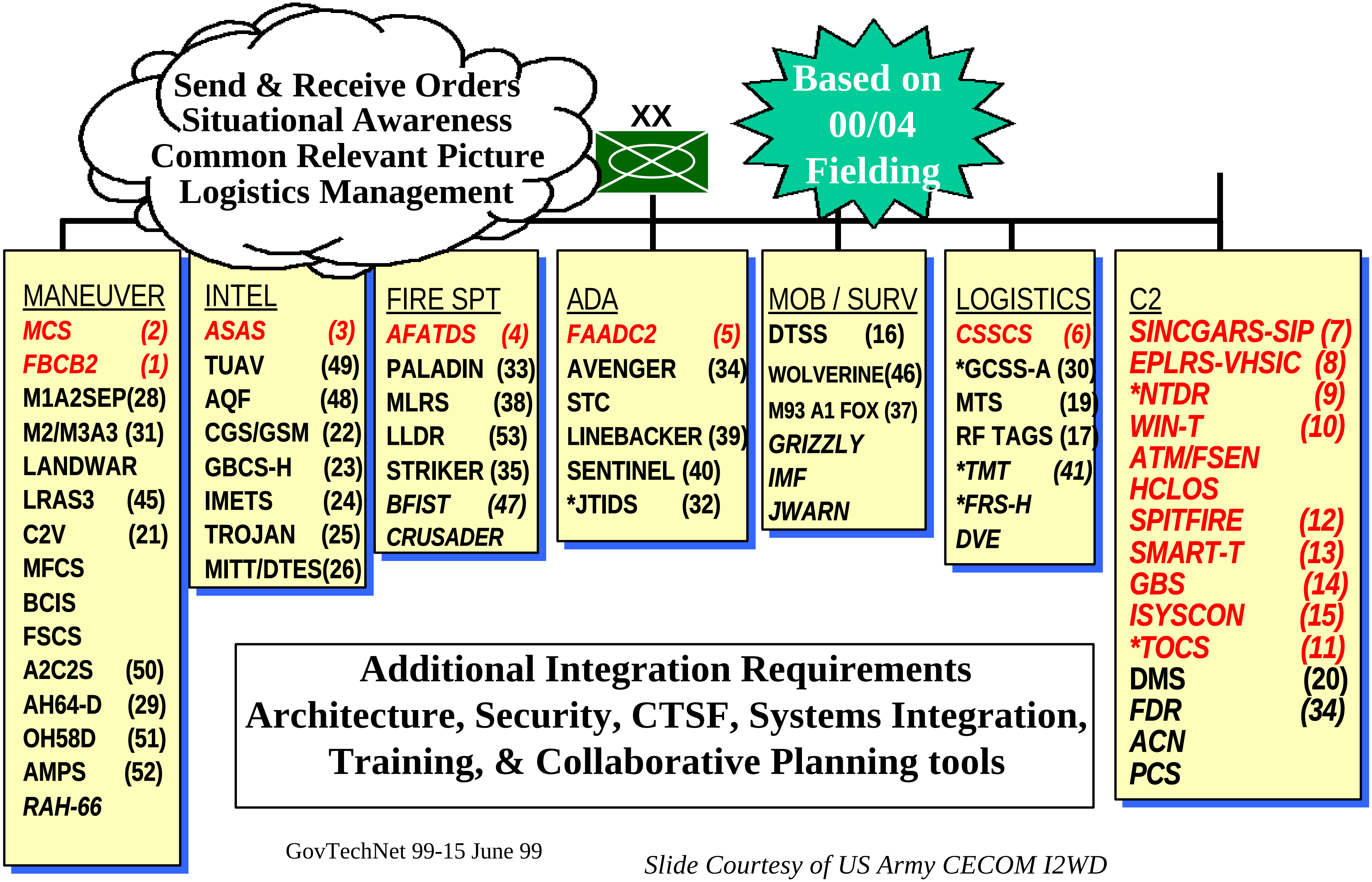
Army XXI - *Into the Future*

The Incorporation of Digital Technology Across All Of Our Battlefield Systems Will Give Commanders And Soldiers Unprecedented Capability to Gather And Share Tactical Information

PROGRAM EXECUTIVE OFFICE COMMAND, CONTROL, AND COMMUNICATIONS SYSTEMS 8/28/97 0005

Slide Courtesy of US Army PEOC3S

U.S. Army Near Term Requirements FDD Division Chart



Send & Receive Orders
Situational Awareness
Common Relevant Picture
Logistics Management

XX

Based on 00/04 Fielding

MANEUVER
- *MCS (2)*
- *FBCB2 (1)*
- M1A2SEP(28)
- M2/M3A3 (31)
- LANDWAR
- LRAS3 (45)
- C2V (21)
- MFCS
- BCIS
- FSCS
- A2C2S (50)
- AH64-D (29)
- OH58D (51)
- AMPS (52)
- *RAH-66*

INTEL
- *ASAS (3)*
- TUAV (49)
- AQF (48)
- CGS/GSM (22)
- GBCS-H (23)
- IMETS (24)
- TROJAN (25)
- MITT/DTES(26)

FIRE SPT
- *AFATDS (4)*
- PALADIN (33)
- MLRS (38)
- LLDR (53)
- STRIKER (35)
- *BFIST (47)*
- *CRUSADER*

ADA
- *FAADC2 (5)*
- AVENGER (34)
- STC
- LINEBACKER (39)
- SENTINEL (40)
- *JTIDS (32)

MOB / SURV
- DTSS (16)
- WOLVERINE(46)
- M93 A1 FOX (37)
- *GRIZZLY*
- *IMF*
- *JWARN*

LOGISTICS
- *CSSCS (6)*
- *GCSS-A (30)
- MTS (19)
- RF TAGS (17)
- **TMT (41)*
- **FRS-H*
- *DVE*

C2
- *SINCGARS-SIP (7)*
- *EPLRS-VHSIC (8)*
- **NTDR (9)*
- *WIN-T (10)*
- *ATM/FSEN*
- *HCLOS*
- *SPITFIRE (12)*
- *SMART-T (13)*
- *GBS (14)*
- *ISYSCON (15)*
- **TOCS (11)*
- DMS (20)
- *FDR (34)*
- *ACN*
- *PCS*

Additional Integration Requirements
Architecture, Security, CTSF, Systems Integration,
Training, & Collaborative Planning tools

GovTechNet 99-15 June 99

Slide Courtesy of US Army CECOM I2WD

U.S. Army Objective Requirements
ABCS Systems/Networks Chart

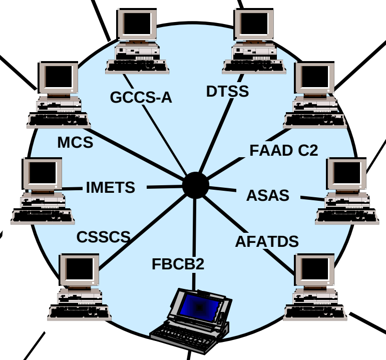
GCCS-A Inerop
AIBS-army-96
FAISA-army-97
IMETS-army-97-98
ISYSCON-army-U
TARSTAT-army-97-98
AMSAA-joint-96
APC-joint-96
ASAS-joint-97
ATCOM-joint-96
AWDS-joint-97
CASCOM-joint-96
CTAPS/TBCMS-joint-97
DAMO-ODR-joint-96
DES-joint-96
DLA/ICIS-joint-96
GCCS/GSORTS-joint-98
GCCS/GSRDI-joint-98
GCCS/JOPES-joint-98
IOC-joint-96
ISC-P-joint-96
JTAV-joint-97
LOGSA-joint-96
MCS-joint-96
PERSCOM-joint-96
RAMS-joint-96
REQVAL-joint-96
SAMAS-joint-96
TAV-joint-96

MCS Interop
AGCCS-army-96
DTSS-army-96
LFCS-army-97
CTAPS-joint-97
JMCIS-joint-98
JStarsCGS-joint-98
TCO-joint-98
AUSTACCS-alliled-98
HEROS-allied-96
LFCCIS-allied-97
QIFS-allied-98
SIACCON-allied-98
SCIF-allied-96

IMETS Interop
GPS-army-
MMS-army-
UAV-army-
JSTARS CGS-joint

CSSCS Interop
DAMM-R-army-99
ICS3-army-99
SAAS/MOD-army-99
SAMS/2-army-99
SARSS/1-army-97
SARSS/2AD-army-98
SIDPERS/2.75-army-97
SIDPERS-3.army-98
SPRS/R-army-97
TAMMIS-army-98
ULLS/S4-army-98

DTSS Interop
FAST-joint-
JSTARS CGS-joint-
MITT-joint-

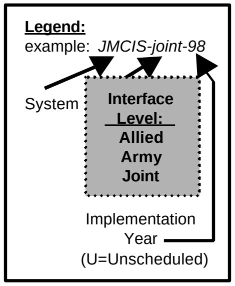


FBCBS Interop
A2C2S-army-99
BCIS-army-
KIOWA-army-U
LVRS-army-U
M1A2 SEP-army-
M2A3-army-
MICAD-
NBCRS-army
Paladin-AFCS
PLGR-army-97
LandWarrior-army

FAAD C2 Interop
LLAPI-allied-95
GBS Radar-army-94
HIMAD-army-94
LSDIS Radar-army-97
TIBS-army-U
AWACS-joint-93
Hawkeye-joint-93

AFATDS Interop
ATHS-army-97
BCS-army-97
FBCB2-army-00
FDS-army-97
Firefinder (q-36)-army-97
FIST DMD-army-97
FOCC-army-97
FOS-army-98
IDM-army-99
IFSAS-army-97
LtacFire-army-97
MBC-army-97
MDS-army-97
MFCS-army-99
MMS-army-97
UAV/TS/00-army-U
AFATDS-joint-99 (MC)
CTAPS/TBMCS-joint-98
IFSAS-joint-97 (MC)
Jstars/CGS-joint-97
TacFire-01-joint-U (MC)
ADLER-allied-98
ATLAS-allied-98
BATES-allied-98

ASAS Interop
Adv Quickfix-army-U
AMS-army-00
ARL-army-U
ATCAE-army-97
CTS/CTAPS-army-97
DAI-army-97
Enhan Trackworl-army-U
EPDS-army-97
ETRAC-army-U
ETUT-army-97
GBCS-army-U
Guardrail-army-97
IEWCS-army-U
IPF-army-97
MIES-army-97
MIIT-army-97
NGIC-army-U
NPIC-army-U
NSA-army-07
SSP/S-army-97
TEAMMATE-army-97
TES-army-97
THMT-army-97
TrafficJam-army97
Trailblazer-army-97
TRRIP-army-U
UAV GCS-army-97
UAV MPCS-army-97
CARS/TRIGS-joint-97
IAC-joint-97
JMCIS-joint-97
JstarsCGS-joint-97
NIPS-joint-97
TBCMS-joint-U
TCAC-joint-97
PASS-K-alllied-U
RAPIDE-allied-97

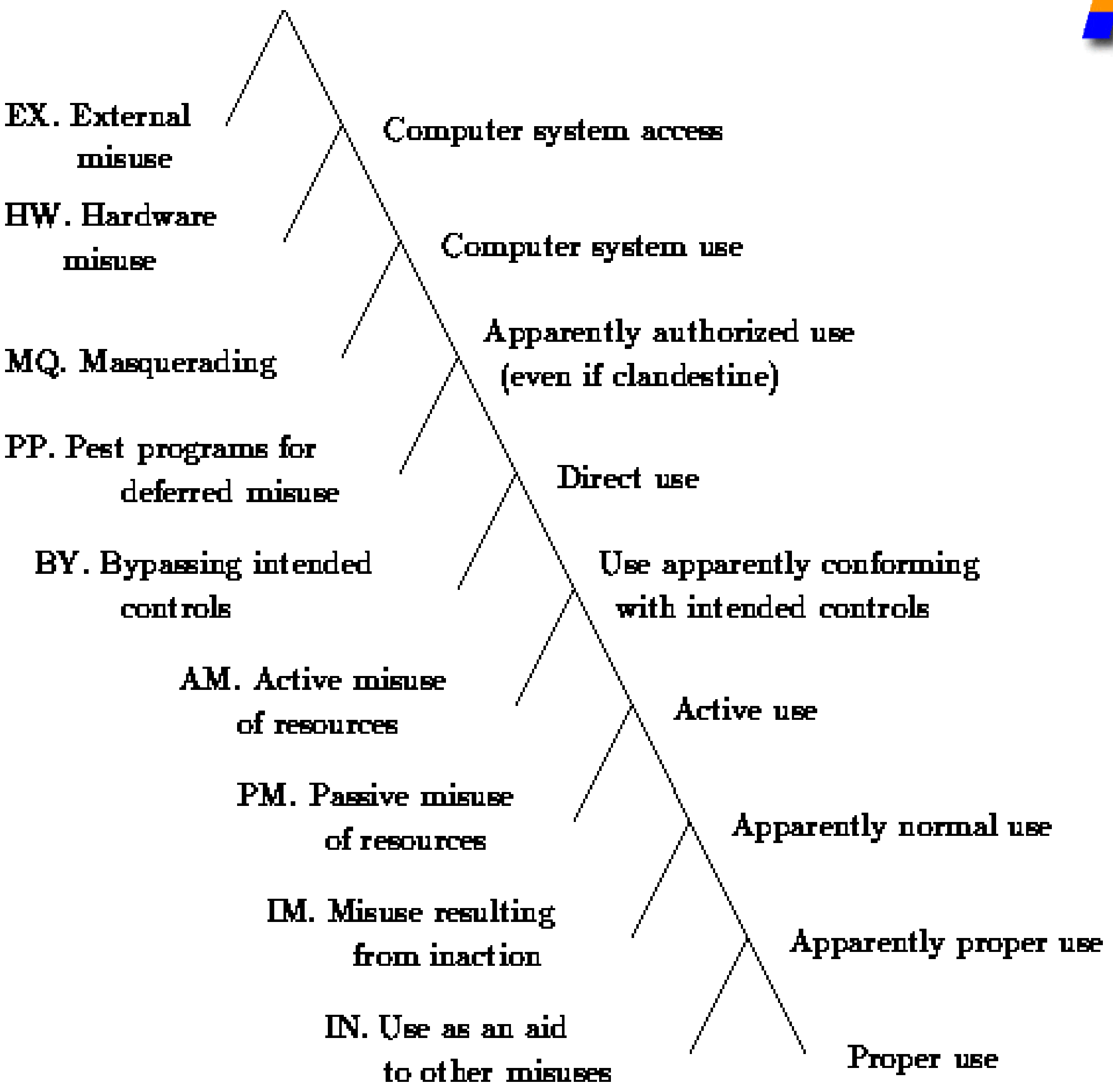

Legend:
example: *JMCIS-joint-98*
System
Interface Level:
Allied
Army
Joint
Implementation Year
(U=Unscheduled)

Slide Courtesy of US Army CECOM I2WD

Partial View to Problem’s Scale

Army Information Systems			**14,544**
– Major Systems		1,219	
• Mission Critical	638		
• Other Major	581		
– Other Systems	(996 Web sites)	13,325	
Information Technology Controlled Devices			**444,196**
– PCs/Servers		365,077	
– Facilities & Other		42,048	
– Communications Hardware/Software		7,071	
Army IS Security Program (total funding)			**$ 87 million**

Classes of Computer Misuse Techniques



EX. External misuse

Computer system access

HW. Hardware misuse

Computer system use

Apparently authorized use (even if clandestine)

MQ. Masquerading

PP. Pest programs for deferred misuse

Direct use

BY. Bypassing intended controls

Use apparently conforming with intended controls

AM. Active misuse of resources

Active use

PM. Passive misuse of resources

Apparently normal use

IM. Misuse resulting from inaction

Apparently proper use

IN. Use as an aid to other misuses

Proper use

Securing Systems at the Desktop

- Insider Misuse
- Development Practice
- Threat is Learning
- Warrior’s “desktop”
- Assurance >> Securing Systems
- Process and Culture

- Holistic interpretation
- Acquisition Strategy
- Education, Training
- Spectrum of Information
- Overarching concept for INFOSURV
- No silver bullets

Directions for INFOSURV R&D

❶ **Robust networking protocols**

❷ **Requirements metrics**

❸ **Predictable systems composition**

❹ **Data analysis and correlation**

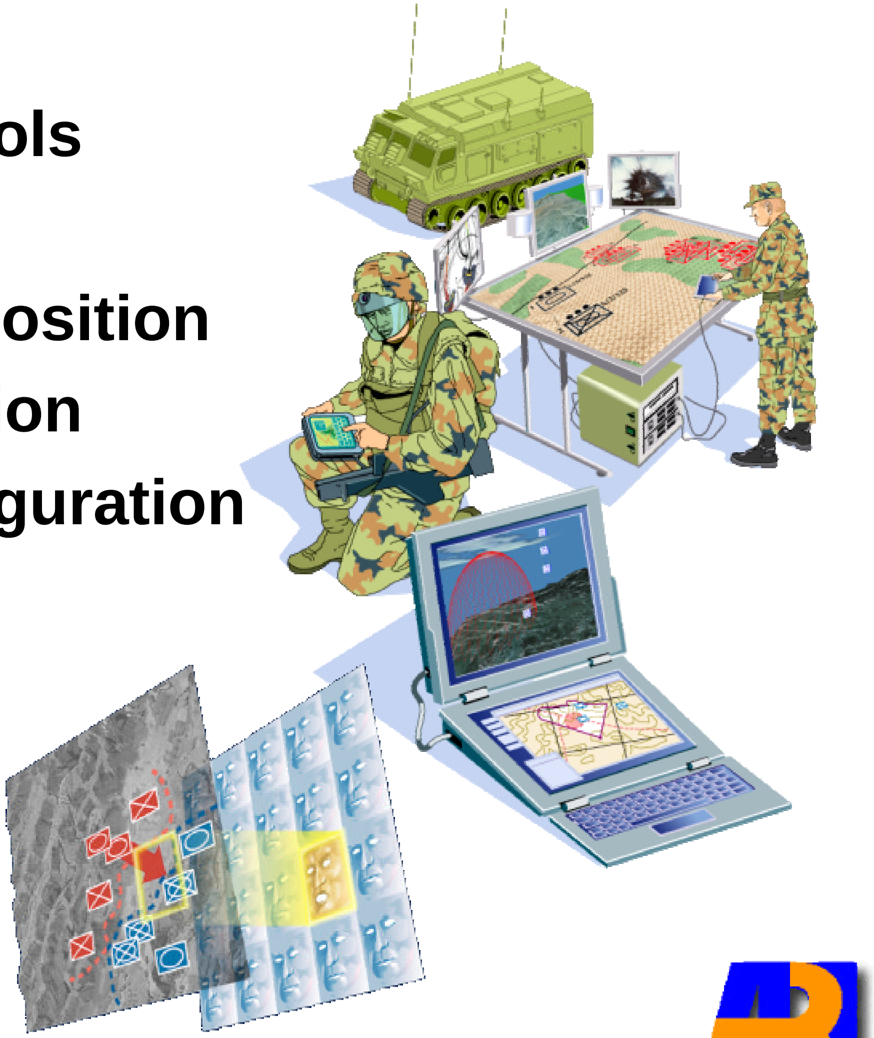
❺ **Dynamic system (re) configuration**

❻ **Dynamic adaptability**

❼ **Architectures**

❽ **Mobile code**

❾ **Components**



INFOSEC Research Areas

1 -Security Engineering Methodologies

2 -Detecting Intrusion and Misuse

3 -Mobile, Foreign Code

4 -Controlled Sharing

5 -Denial of Service

6 -Application Security

7 -Communications Security

8 -Security in Mobile Environments

9 -Security Management Infrastructure